Relatório Anual PTSOC 2023

"Ano do Ransomware"

Índice

CAPÍTULO 1

1.

Enquadramento

Em 2023, num contexto global em que os incidentes de cibersegurança e o cibercrime continuam a aumentar em número e em sofisticação, com o ransomware, as burlas online e as técnicas de engenharia social como phishing, smshing e mais recentemente o quishing, com a utilização de QRCodes, a liderar o quadro de ameaças do ciberespaço. Estas técnicas amplificadas pelos avanços da Inteligência Artificial (IA) e do machine-learning (ML), irão permitir analisar e processar grandes volumes de dados, em tempo real, automatizando e introduzindo maior sofisticação nestas tipologias de ataques.

Esta tendência é reforçada no Relatório de Riscos Globais de 2023 do World Economic Forum que antecipa a generalização do cibercrime e a insegurança cibernética como dois dos 10 principais riscos mundiais nos próximos anos e eleva a ciber(in)segurança como um dos principais assuntos a endereçar pela Comunidade Europeia na agenda da Década Digital para 2030 da União Europeia (UE).

Este relatório anual do PTSOC, pretende apresentar uma breve súmula dos principais acontecimentos e tendências que se observaram em 2023 nos domínios da cibersegurança e colocar em perspetiva os principais desafios que se antecipam para 2024.

CAPÍTULO 2

2.

Grandes ciberataques de 2023

janeiro

O **Royal Mail**, empresa postal britânica, foi alvo de um ciberataque de **ransomware**, que levou à interrupção, por mais de uma semana, do **envio internacional de encomendas e cartas** causando um impacto significativo nas suas operações.

fevereiro

O grupo **Super Bock**, foi alvo de um ciberataque de **ransomware** que provocou constrangimentos nas operações de **abastecimento** de alguns dos seus produtos no mercado comercial.

março

A página de Internet da **Assembleia Nacional Francesa** foi alvo de um **ataque de DDoS** por um grupo de 'hackers' pró-russos **causando a sua indisponibilidade temporária**.

abril

Colaboradores da **Samsung**, de forma não intencional, **expuseram código interno e notas de reuniões internas** ao utilizar a ferramenta **'ChatGPT' da OpenAI** para os ajudar na identificação de erros e produção dos resumos das reuniões.

O **Instituto Politécnico de Leiria** sofreu um ataque informático que fez com que 14 mil alunos ficassem sem acesso à internet nas escolas e residenciais. Este ataque, acabou por provocar instabilidade nos seus serviços nomeadamente a **indisponibilidade de toda a atividade online da instituição**.

maio

O **GlobalCaja**, sediado na cidade espanhola de Albacete, foi alvo de um ataque informático (Ransomware) que **bloqueou diversos escritórios e ocorreu a exfiltração de dados confidenciais, documentos de clientes e colaboradores, passaportes e contratos**. O grupo Play ransomware reinvidicou a autoria do ataque.

junho

A **NATO** sofreu uma campanha de phishing com foco ao Nato Summit que aconteceu em Vilnius, Lituânia, nos dias 11 e 12 de julho. Este ataque informático utilizou **técnicas de typosquatting e emails de spear-phishing** com o objetivo de infetar os participantes com malware.

julho

Diversos bancos italianos sofreram ataques de DDoS. A agência de cibersegurança nacional, em Itália confirmou que pelo menos cinco entidades bancárias italianas foram alvos de ciberataques. Estes ataques **provocaram indisponibilidade nos sites destas entidades bancárias, ficando inacessíveis**. O grupo pró-russo NoName foi identificado pelas autoridades italianas como tendo sido os atores maliciosos responsáveis por estes ataques.

agosto

setembro

O município de Gondomar, no dia 27 de setembro foi alvo de um ciberataque, obrigando as autoridades a colocarem os sistemas offline e a contactarem o Centro Nacional de Cibersegurança e a Comissão Nacional de Proteção de Dados. O gangue de ransomware Rhysida, autor do ciberataque, divulgou passaportes e documentos financeiros após o resgate não ter sido pago.

outubro

A empresa de teste de ADN **23andMe**, reportou em outubro o acesso não autorizado a dados biométricos de 5.5 milhões de clientes. Os atores maliciosos utilizaram contas previamente comprometidas para realizar um ataque de "***credential stuffing***". Este tipo de ataque poderia ter sido evitado pelos clientes através da não reutilização de passwords. Este incidente trouxe também ao de cima a necessidade de as empresas proactivamente analisarem a segurança das contas dos seus utilizadores.

novembro

A multinacional norte-americana de desenvolvimento aeroespacial e de defesa, **Boeing**, sofreu um incidente de cibersegurança pelo gangue de ransomware LockBit onde cerca de 43 GB de dados foram publicados online. O incidente não apresentou ameaças às aeronaves ou a segurança da aviação.

dezembro

A 10 de dezembro, a **easypark**, empresa de estacionamento de veículos, divulgou que foi alvo de um ataque informático onde os atores maliciosos tiveram acesso a informação pessoal dos seus clientes como, o nome, número de telemóvel, morada, email e o número parcial do cartão de débito/crédito. Apesar do incidente, a empresa agiu de forma rápida e acertada, alterando a palavra-passe e notificando os seus clientes e as autoridades competentes em tempo útil.

CAPÍTULO 3

3.

Principais ciberameaças em 2023

Ransomware

O ano 2023, ficou marcado pelo crescimento da oferta de serviços do tipo Ransomware-as-a-Service (RaaS). Este modelo de negócio, tornou-se particularmente lucrativo e os grupos cibercriminosos têm-se dedicado cada vez mais a esta atividade tornando este tipo de serviços cada vez mais acessível a qualquer pessoa. Em 2023, assistimos a uma nova tática de extorção, onde o ator malicioso ameaça reportar a vítima através das diligências legais, após a mesma ter sido comprometida e não ter reportado às autoridades competentes.

Engenharia Social

A engenharia social foi a técnica de ataque que mais prevaleceu em 2023. A utilização destas técnicas explora o interesse, a preocupação, a curiosidade e o medo das pessoas, principalmente através do e-mail, para obter informação confidencial como por exemplo credenciais de acesso. Esta é a técnica favorita dos cibercriminosos para o acesso inicial às redes internas das organizações. Infelizmente, muitos e-mails com conteúdo malicioso, especialmente URLs, ainda passam por filtros básicos de e-mail e acabam por ser enviados aos utilizadores.

DoS/DDoS

O DDoS é uma das ciberameaças mais impactantes, causando indisponibilidade dos serviços ou diminuindo o seu desempenho. Em 2023, a utilização de Botnets ou mesmo o crescimento de serviços DDoS-for-Hire fizeram aumentar o número de ataques de negação de serviço como também a sua volumetria. Ainda neste ano, foi reportado o maior ataque DDoS de que há registo, tendo tido como alvo os serviços da Google.

Tentativa de Login

Devido à resistência à utilização do duplo fator de autenticação, a tentativa de login continuou a ser um dos ataques mais comuns em 2023. As tentativas de login/ ataques de força bruta utilizam a técnica de tentativa e erro para adivinhar as informações de login da vítima. Os atores maliciosos utilizam todas as combinações possíveis para obter acesso à conta em questão.

CAPÍTULO 4

O que vimos no .PT em 2023

Principais Indicadores

164
Eventos Reportados
(canal público)

8% ~330k
E-mails maliciosos recebidos

647
Casos DNS Abuse: identificados

130
Casos DNS Abuse: reportados

89%
Casos DNS Abuse: Phishing

82%
Casos DNS Abuse mitigados
(menos de 8 dias)

Implementação Standards Segurança em Registrars

Web

22.9%
Registrars com
DNSSEC na página

94.3%
Registrars com Certificado
Digital Válido na Página

94.3%
Registrars com
HTTPS na Página

85.7%
Registrars com HTTPS
Redirect na Página

35.3%
Registrars com
HSTS na Página

2.9%
Registrars com
DANE na Página

O PTSOC – Centro de Operações de Segurança do .PT – realizou um estudo sobre a implementação dos principais standards de segurança nas vertentes web e email nas plataformas disponibilizadas pelos Registrars .PT.

Implementação Standards Segurança em Registrars

E-mail

14.3%
Registrars com
DNSSEC no E-mail

85.7%
Registrars com
SPF no E-mail

68.6%
Registrars com
DKIM no E-mail

62.9%
Registrars com
DMARC no E-mail

Webcheck

20.9% ↑
Páginas web testadas com DNSSEC

81.007
Testes realizados

71.2% ↑
Páginas web testadas com HTTPS

8.1% ↓
Páginas web testadas com HSTS

50.2% ↑
Correio electrónico testado com SPF

44.5% ↑
Correio electrónico testado com STARTTLS

Formação & Sensibilização

5
Cursos cibersegurança

3239
Pessoas impactadas

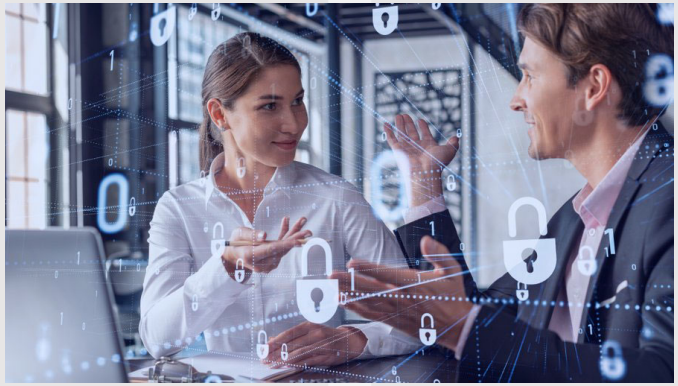
7
Edições da PTSOC {Digest}

4
Edições da PTSOC {News}

16
Workshops PTSOC

673
Pessoas impactadas

Formação disponível



[Mooc “Gestão dos Riscos de Cibersegurança nas Organizações”]

[Mooc “Gestão da Continuidade de Negócio”]

CAPÍTULO 5

5.

Para onde olhar em 2024

"O ransomware-as-a-service (RaaS) tornou-se um negócio próspero"

Ransomware é um dos ciberataques mais lucrativos do momento. Em 2024, o modelo RaaS continuará a ter um crescimento contínuo, pois provou ser um veículo incrivelmente eficiente para maximizar os lucros resultantes de ataques do tipo ransomware. Embora a trajetória de crescimento permaneça a mesma, o alvo principal dos ataques de ransomware não. O envolvimento dos governos, entidades governamentais e de segurança na defesa das infraestruturas críticas, motivará os grupos de ransomware a direcionar a mira para as pequenas e médias empresas.

Para onde olhar em 2024

"O advento dos ataques através de Supply Chain"

Os atacantes procuram sempre ligações de confiança e que lhes permitam obter acesso às redes dos alvos causando o menor ruído possível.

Os ataques de Supply Chain ocorrem quando os atacantes se infiltram nos sistemas por meio de um parceiro ou fornecedor de serviços com acessos privilegiados às redes do alvo.

Este será um dos principais vetores de ataque que se perspetiva para 2024, sendo um dos temas a ter de ser endereçado pelas organizações essenciais com a entrada em vigor de diplomas como a NIS 2.

Para onde olhar em 2024

“A engenharia social indistinguível da realidade”

A engenharia social é um dos problemas de segurança mais difíceis de resolver porque nenhuma ação de conformidade, governo ou gestão de risco pode resolver o facto de que as pessoas serem imperfeitas e suscetíveis a serem enganadas.

O acesso a tecnologias de Inteligência Artificial e Machine Learning para manipulação de áudio e vídeo, irão permitir com facilidade criar conteúdos tão realistas que serão cada vez mais difíceis de distinguir da realidade.

O reforço de campanhas de Awareness nas organizações vão ser fundamentais, ainda assim, será necessária a implementação de mais meios para limitar o impacto destes ataques utilizando princípios de Zero Trust.

Referências

1 | Observatório de Cibersegurança, Relatório Riscos e Conflitos de 2023
https://www.cncs.gov.pt/docs/rel-riscosconflitos2023-obcibercncs.pdf

2 | ENISA Threat Landscape 2023
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

3 | Significant Cyber Incidents
https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

4 | DAN GOODIN, Ransomware group reports victim it breached to SEC regulators
https://arstechnica.com/security/2023/11/ransomware-group-reports-victim-it-breached-to-sec-regulators/

5 | Google
https://cloud.google.com/blog/products/identity-security/goole-cloud-mitigated-largest-ddos-attack-peaking-above-398-million-rps

ptsoc

Produção: janeiro 2024
Grafismo: .pt